

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-116534

(43)Date of publication of application : 02.05.1997

(51)Int.Cl.

H04L 9/32

G06F 13/00

G06F 15/00

H04L 9/14

(21)Application number : 07-271578

(71)Applicant : FUJITSU LTD

(22)Date of filing : 19.10.1995

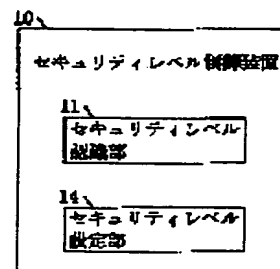
(72)Inventor : KURODA YASUTSUGU

(54) SECURITY LEVEL CONTROLLER AND NETWORK COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To conduct communication without deciding a security level in advance with a communication destination by providing a security level setting section that sets a security level recognized by a security level recognition section as a security level at a security level controller.

SOLUTION: A security level controller 10 is provided with a security level recognition section 11 and a security level setting section 14. The security level recognition section 11 recognizes a security level informed by a communication destination. The security level setting section 14 sets the security level recognized by the security level recognition section 11 as a security level of the security level controller 10. Then the security level of the communication destination recognized by the security level recognition section 11 is set for the security level of the security level controller 10.



LEGAL STATUS

[Date of request for examination] 29.08.2001

[Date of sending the examiner's decision of rejection] 17.08.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2004-19344

[Date of requesting appeal against examiner's decision of rejection] 16.09.2004

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-116534

(43) 公開日 平成9年(1997)5月2日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/32			H 0 4 L 9/00	6 7 3 B
G 0 6 F 13/00	3 5 7		G 0 6 F 13/00	3 5 7 Z
	15/00	3 3 0		15/00 3 3 0 A
H 0 4 L 9/14			H 0 4 L 9/00	6 4 1

審査請求 未請求 請求項の数12 O L (全 17 頁)

(21) 出願番号 特願平7-271578

(22) 出願日 平成7年(1995)10月19日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 黒田 康嗣

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74) 代理人 弁理士 遠山 勉 (外1名)

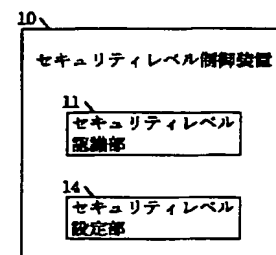
(54) 【発明の名称】 セキュリティレベル制御装置及びネットワーク通信システム

(57) 【要約】

【課題】 通信先との間で予めセキュリティレベルを決定しておくことなく、通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第1の課題とする。

【解決手段】 セキュリティレベル制御装置は、通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部11と、セキュリティレベル認識部11で認識されたセキュリティレベルをセキュリティレベル制御装置10側のセキュリティレベルとして設定するセキュリティレベル設定部14とを備えて構成した。

本発明の第1のセキュリティレベル制御装置に対応した原理ブロック図



【特許請求の範囲】

【請求項1】 通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置において、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

前記セキュリティレベル認識部で認識されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを備えたことを特徴とするセキュリティレベル制御装置。

【請求項2】 通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置において、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、

前記セキュリティレベル認識部で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部と、

前記セキュリティレベル読出部から読み出されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを備えたことを特徴とするセキュリティレベル制御装置。

【請求項3】 セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、

前記クライアント装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

前記セキュリティレベル認識部で認識されたセキュリティレベルを前記クライアント装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを特徴とするネットワーク通信システム。

【請求項4】 セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、

前記サーバ装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

前記セキュリティレベル認識部で認識されたセキュリティレベルを前記サーバ装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを

特徴とするネットワーク通信システム。

【請求項5】 前記サーバ装置は複数設けられており、前記クライアント装置に設けられた前記セキュリティレベル制御装置は、各々のサーバ装置毎にセキュリティレベルを制御することを特徴とする請求項3に記載のネットワーク通信システム。

【請求項6】 前記クライアント装置は複数設けられており、

前記サーバ装置に設けられた前記セキュリティレベル制御装置は、各々のクライアント装置毎にセキュリティレベルを制御することを特徴とする請求項4に記載のネットワーク通信システム。

【請求項7】 前記クライアント装置が有する前記セキュリティレベル制御装置は、

2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、

前記セキュリティレベル認識部で認識された前記サーバ装置のセキュリティレベル及び前記クライアント装置のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部とを有し、

前記セキュリティレベル設定部は、前記セキュリティレベル読出部から読み出されたセキュリティレベルを前記クライアント装置側のセキュリティレベルとして設定することを特徴とする請求項3又は請求項5に記載のネットワーク通信システム。

【請求項8】 前記サーバ装置が有する前記セキュリティレベル制御装置は、

2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、

前記セキュリティレベル認識部で認識された前記クライアント装置のセキュリティレベル及び前記サーバ装置のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部とを有し、

前記セキュリティレベル設定部は、前記セキュリティレベル読出部から読み出されたセキュリティレベルを前記サーバ装置側のセキュリティレベルとして設定することを特徴とする請求項4又は請求項6に記載のネットワーク通信システム。

【請求項9】 前記クライアント装置が有する前記セキュリティレベル制御装置は、前記クライアント装置の要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項7に記載のネットワーク通信システム。

【請求項10】 前記サーバ装置が有する前記セキュリ

ティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項 8 に記載のネットワーク通信システム。

【請求項 11】 セキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムにおいて、

前記サーバ装置及び前記クライアント装置は、セキュリティレベル制御装置を有し、このセキュリティレベル制御装置は、

通信先が通知してくるセキュリティレベルを認識するセキュリティレベル認識部と、

2 組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納したセキュリティレベル変換テーブル部と、

前記セキュリティレベル認識部で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部から読み出すセキュリティレベル読出部と、

前記セキュリティレベル読出部から読み出されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するセキュリティレベル設定部とを有することを特徴とするネットワーク通信システム。

【請求項 12】 前記クライアント装置が有する前記セキュリティレベル制御装置は、前記クライアント装置の要求に従って、通信途中でも、セキュリティレベルを動的に変化させ、

前記サーバ装置が有する前記セキュリティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させることを特徴とする請求項 11 に記載のネットワーク通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、セキュリティレベル制御装置、特に通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置に関する。

【0002】 また、本発明は、ネットワーク通信システム、特にセキュリティレベルが設定された通信を行うサーバ装置及びクライアント装置が設けられたネットワーク通信システムに関する。

【0003】

【従来の技術】 分散して設置されている計算機を相互に接続することにより、電子メール等のサービスを提供するネットワークサービスが商用化されている。

【0004】 ところが、インターネットに代表されるように学術目的で構築されてきたネットワークでは、ネッ

トワークセキュリティに関する考慮が十分にされていない。そのため、ネットワークサービスに対して盗聴、改竄、なりすまし等が行われ問題となっている。

【0005】 ここで、電子メールを例に取り、盗聴、改竄、なりすましについて説明する。盗聴とは、平文、即ち何も暗号化されていない状態の通信文（メッセージ）が配送途中で読まれてしまうことをいう。

【0006】 改竄とは、配送途中で電子メールの内容が変更されてしまうことをいう。改竄は、電子メールが複数の中継ノードを経由して配送される場合に、途中の中継ノードで行われる。

【0007】 なりすましとは、発信者を特定する情報が保護されていない場合に、悪意を持つ第三者が発信者情報を偽造して他人になりすますことをいう。このような問題を解決するため、メッセージ（データ）を暗号化すること、電子署名を用いて改竄を防ぐこと、ユーザ（通信相手）を認証することなどが単独あるいは組み合わせられて行われている。また、サーバ及びクライアントの形態を持つネットワーク通信では、サーバ装置を認証することやクライアント装置を認証することも行われている。

【0008】 ここで、暗号化技術としては、秘密鍵暗号方式や公開鍵暗号化方式等が知られている。秘密鍵暗号化方式では、通信の当事者間で共通の鍵を使って暗号化と復号化を行う。一方、公開鍵暗号化方式は、各人の秘密鍵と公開鍵の組み合わせで構成され、他者には公開鍵を知らせ、秘密鍵は自分一人だけが知っている方式である。この方式では、公開鍵で暗号化されたものは秘密鍵で解くことができる。例えば、A から B へ送信するときには、A は B の公開鍵で暗号化を行い、受け取った B は自分の秘密鍵でこれを解く。この暗号文を解けるのは、自分の秘密鍵を知る B だけである。

【0009】 また、認証技術については、パスワード認証、公開鍵方式を用いた電子署名等が知られている。

【0010】

【発明が解決しようとする課題】 前記従来の技術において、ネットワークサービスに対して盗聴、改竄、なりすまし等を防止するため、どのような処理を組み合わせるかににより、複数のセキュリティレベルが生じることになる。

【0011】 例えば、電子メールを暗号化することだけでなく、電子メールを暗号化すると同時にユーザ認証を行う方がセキュリティレベルが高いと考えられる。セキュリティを強化することだけを考えれば、より多くの処理を組み合わせた方が安全ではあるが、その場合に負荷が高くなるのも事実である。

【0012】 そこで、通信内容の重要性を反映させたセキュリティレベルを設定することが適切であると考えられるが、メッセージの重要性に基づいて適切なセキュリティレベルを設定することを「セキュリティのポリシ

一」という。

【0013】ところで、前記従来の技術においては、この「セキュリティのポリシー」に関して下記のような問題が生じている。第1の問題は、通信先との間で予め決められたセキュリティのポリシーでしか通信できず、それ以外のポリシーでは通信できないことである。

【0014】第2の問題は、通信先のセキュリティレベルが常に優先され、自分のセキュリティレベルを反映できないことである。本発明は、このような事情に鑑みてなされたもので、通信先との間で予めセキュリティレベルを決定しておくことなく通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第1の課題とする。

【0015】また、本発明は、自分のセキュリティレベルを反映させた通信を行うことを可能とするセキュリティレベル制御装置及びネットワーク通信システムを提供することを第2の課題とする。

【0016】

【課題を解決するための手段】

《本発明の第1のセキュリティレベル制御装置10》本発明の第1のセキュリティレベル制御装置10は、前述した第1の課題を解決するため以下のように構成されている（請求項1に対応）。図1は、本発明のセキュリティレベル制御装置10に対応した原理ブロック図である。

【0017】即ち、通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置10において、セキュリティレベル認識部11及びセキュリティレベル設定部14を備えて構成されている。

【0018】（セキュリティレベル認識部11）前記セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。

【0019】（セキュリティレベル設定部14）前記セキュリティレベル設定部14は、前記セキュリティレベル認識部11で認識されたセキュリティレベルをセキュリティレベル制御装置10側のセキュリティレベルとして設定する。

【0020】本発明の第1のセキュリティレベル制御装置10によれば、下記的作用が行われる。まず、セキュリティレベル認識部11で認識された通信先のセキュリティレベルが、セキュリティレベル制御装置10側のセキュリティレベルとして設定される。

【0021】《本発明の第2のセキュリティレベル制御装置10》本発明の第2のセキュリティレベル制御装置10は、前述した第2の課題を解決するため以下のように構成されている（請求項2に対応）。図1は、本発明のセキュリティレベル制御装置10に対応した原理ブロック図である。

【0022】即ち、通信先との間で行われる通信のセキュリティレベルを制御するセキュリティレベル制御装置

10において、セキュリティレベル認識部11、セキュリティレベル変換テーブル部12、セキュリティレベル読出部13及びセキュリティレベル設定部14を備えて構成されている。

【0023】（セキュリティレベル認識部11）前記セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。

【0024】（セキュリティレベル変換テーブル部12）前記セキュリティレベル変換テーブル部12は、2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【0025】（セキュリティレベル読出部13）前記セキュリティレベル読出部13は、前記セキュリティレベル認識部11で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置10側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部12から読み出す。

【0026】（セキュリティレベル設定部14）前記セキュリティレベル設定部14は、前記セキュリティレベル読出部13から読み出されたセキュリティレベルをセキュリティレベル制御装置10側のセキュリティレベルとして設定する。

【0027】本発明の第2のセキュリティレベル制御装置10によれば、下記的作用が行われる。まず、セキュリティレベル認識部11で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置10側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部12から読み出される。そして、この読み出されたセキュリティレベルがセキュリティレベル装置10側のセキュリティレベルとして設定される。

【0028】《本発明の第1のネットワーク通信システム》本発明の第1のネットワーク通信システムは、前述した第1の課題を解決するため以下のように構成されている（請求項3に対応）。図3は、本発明の第1のネットワーク通信システムに対応した原理ブロック図である。

【0029】即ち、セキュリティレベルが設定された通信を行うサーバ装置20及びクライアント装置30が設けられたネットワーク通信システムにおいて、前記クライアント装置30は、セキュリティレベル制御装置10を有する。そして、このセキュリティレベル制御装置10は、セキュリティレベル認識部11及びセキュリティレベル設定部14を備えて構成されている。

【0030】（セキュリティレベル認識部11）前記セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。

【0031】（セキュリティレベル設定部14）前記セキュリティレベル設定部14は、前記セキュリティレベル認識部11で認識されたセキュリティレベルを前記クライアント装置30側のセキュリティレベルとして設定する。

【0032】本発明の第1のネットワーク通信システムによれば、クライアント装置30側において、下記的作用が行われる。まず、セキュリティレベル認識部11で認識されたサーバ装置20のセキュリティレベルが、クライアント装置30側のセキュリティレベルとして設定される。

【0033】《本発明の第2のネットワーク通信システム》本発明の第2のネットワーク通信システムは、前述した第1の課題を解決するため以下のように構成されている（請求項4に対応）。図4は、本発明の第2のネットワーク通信システムに対応した原理ブロック図である。

【0034】即ち、セキュリティレベルが設定された通信を行うサーバ装置20及びクライアント装置30が設けられたネットワーク通信システムにおいて、前記サーバ装置20は、セキュリティレベル制御装置10を有する。そして、このセキュリティレベル制御装置10は、セキュリティレベル認識部11及びセキュリティレベル設定部14を備えて構成されている。

【0035】（セキュリティレベル認識部11）前記セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。

【0036】（セキュリティレベル設定部14）前記セキュリティレベル設定部14は、前記セキュリティレベル認識部11で認識されたセキュリティレベルを前記サーバ装置20側のセキュリティレベルとして設定する。

【0037】本発明の第2のネットワーク通信システムによれば、サーバ装置20側において、下記的作用が行われる。まず、セキュリティレベル認識部11で認識されたクライアント装置30のセキュリティレベルがサーバ装置20側のセキュリティレベルとして設定される。

【0038】《本発明の第3のネットワーク通信システム》本発明の第3のネットワーク通信システムは、前述した第1の課題を解決するため以下のように構成されている（請求項5に対応）。

【0039】即ち、第1のネットワーク通信システムにおいて、前記サーバ装置20は複数設けられている。そして、前記クライアント装置30に設けられた前記セキュリティレベル制御装置10は、各々のサーバ装置20毎にセキュリティレベルを制御する。

【0040】本発明の第3のネットワーク通信システムによれば、下記的作用が行われる。、即ち、各々のサーバ装置20毎にセキュリティレベルが制御される。

《本発明の第4のネットワーク通信システム》本発明の第4のネットワーク通信システムは、前述した第1の課題

を解決するため以下のように構成されている（請求項6に対応）。

【0041】即ち、第2のネットワーク通信システムにおいて、前記クライアント装置30は複数設けられている。そして、前記サーバ装置20に設けられた前記セキュリティレベル制御装置10は、各々のクライアント装置30毎にセキュリティレベルを制御する。

【0042】本発明の第4のネットワーク通信システムによれば、下記的作用が行われる。即ち、各々のクライアント装置30毎にセキュリティレベルが制御される。

《本発明の第5のネットワーク通信システム》本発明の第5のネットワーク通信システムは、前述した第2の課題を解決するため以下のように構成されている（請求項7に対応）。

【0043】即ち、第1又は第3のネットワーク通信システムにおいて、前記クライアント装置30が有する前記セキュリティレベル制御装置10は、セキュリティレベル変換テーブル部12及びセキュリティレベル読出部13を有する。

【0044】セキュリティレベル変換テーブル部12は、2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【0045】セキュリティレベル読出部13は、前記セキュリティレベル認識部11で認識された通信先のセキュリティレベル及び前記クライアント装置30側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部12から読み出す。

【0046】そして、前記セキュリティレベル設定部14は、前記セキュリティレベル読出部13から読み出されたセキュリティレベルを前記クライアント装置30側のセキュリティレベルとして設定する。

【0047】本発明の第5のネットワーク通信システムによれば、下記的作用が行われる。まず、セキュリティレベル認識部11で認識されたサーバ装置20のセキュリティレベル及びクライアント装置30のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部12から読み出される。そして、この読み出されたセキュリティレベルがクライアント装置30側のセキュリティレベルとして設定される。

【0048】《本発明の第6のネットワーク通信システム》本発明の第6のネットワーク通信システムは、前述した第2の課題を解決するため以下のように構成されている（請求項8に対応）。

【0049】即ち、第2又は第4のネットワーク通信システムにおいて、前記サーバ装置20が有する前記セキュリティレベル制御装置10は、セキュリティレベル変換テーブル部12及びセキュリティレベル読出部13を

有する。

【0050】セキュリティレベル変換テーブル部12は、2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【0051】セキュリティレベル読出部13は、前記セキュリティレベル認識部11で認識された前記クライアント装置30のセキュリティレベル及び前記サーバ装置20側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部12から読み出す。

【0052】そして、前記セキュリティレベル設定部14は、前記セキュリティレベル読出部13から読み出されたセキュリティレベルを前記サーバ装置20のセキュリティレベルとして設定する。

【0053】本発明の第6のネットワーク通信システムによれば、下記的作用が行われる。まず、セキュリティレベル認識部11で認識されたクライアント装置30のセキュリティレベル及びサーバ装置20側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部12から読み出される。そして、この読み出されたセキュリティレベルがサーバ装置20側のセキュリティレベルとして設定される。

【0054】《本発明の第7のネットワーク通信システム》本発明の第7のネットワーク通信システムは、前述した第2の課題を解決するため以下のように構成されている（請求項9に対応）。

【0055】即ち、第5のネットワーク通信システムにおいて、前記クライアント装置30が有する前記セキュリティレベル制御装置10は、前記クライアント装置30の要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【0056】本発明の第7のネットワーク通信システムによれば、下記的作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

《本発明の第8のネットワーク通信システム》本発明の第8のネットワーク通信システムは、前述した第2の課題を解決するため以下のように構成されている（請求項10に対応）。

【0057】即ち、第6のネットワーク通信システムにおいて、前記サーバ装置が有する前記セキュリティレベル制御装置は、前記サーバ装置からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【0058】本発明の第8のネットワーク通信システムによれば、下記的作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

《本発明の第9のネットワーク通信システム》本発明の第9のネットワーク通信システムは、前述した第2の課題

を解決するため以下のように構成されている（請求項11に対応）。図5は、第9のネットワーク通信システムに対応した原理ブロック図である。

【0059】即ち、セキュリティレベルが設定された通信を行うサーバ装置20及びクライアント装置30が設けられたネットワーク通信システムにおいて、前記サーバ装置20及び前記クライアント装置30は、セキュリティレベル制御装置10を有する。このセキュリティレベル制御装置10は、セキュリティレベル認識部11、セキュリティレベル変換テーブル部12、セキュリティレベル読出部13及びセキュリティレベル設定部14を備えて構成されている。

【0060】（セキュリティレベル認識部11）前記セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。

【0061】（セキュリティレベル変換テーブル部12）前記セキュリティレベル変換テーブル部12は、2組のセキュリティレベルからなるインデックスと実際に行われる通信のセキュリティレベルとの対応関係を格納する。

【0062】（セキュリティレベル読出部13）前記セキュリティレベル読出部13は、前記セキュリティレベル認識部11で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置10側のセキュリティレベルを前記インデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部12から読み出す。

【0063】（セキュリティレベル設定部14）前記セキュリティレベル設定部14は、前記セキュリティレベル読出部13から読み出されたセキュリティレベルをセキュリティレベル制御装置10側のセキュリティレベルとして設定する。

【0064】本発明の第9のネットワーク通信システムによれば、下記的作用が行われる。まず、セキュリティレベル認識部11で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置10側のセキュリティレベルがインデックスとされる。そして、このインデックスに対応するセキュリティレベルがセキュリティレベル変換テーブル部12から読み出される。そして、この読み出されたセキュリティレベルがセキュリティレベル装置10側のセキュリティレベルとして設定される。

【0065】《本発明の第10のネットワーク通信システム》本発明の第10のネットワーク通信システムは、前述した第2の課題を解決するため以下のように構成されている（請求項12に対応）。

【0066】即ち、第9のネットワーク通信システムにおいて、前記クライアント装置30が有する前記セキュリティレベル制御装置10は、前記クライアント装置30の要求に従って、通信途中でも、セキュリティレベル

を動的に変化させる。

【0067】そして、前記サーバ装置20が有する前記セキュリティレベル制御装置10は、前記サーバ装置20からの要求に従って、通信途中でも、セキュリティレベルを動的に変化させる。

【0068】本発明の第10のネットワーク通信システムによれば、下記の作用が行われる。即ち、通信途中でも、セキュリティレベルを動的に変化させる。

【0069】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

（実施形態のシステム構成）実施形態のシステムは、図6に示すように、サーバ装置20（サーバとも言う）、このサーバ装置に接続されたネットワーク40、及び、このネットワーク40に接続されたクライアント装置30（クライアントともいう）を備えて構成されている。

【0070】このシステムでは、サーバ装置20とクライアント装置30との間で通信が行われる。この通信では、盗聴、改竄、なりすまし等を防止するため、通信内容の重要性に応じて5段階のセキュリティレベルを設定することが可能となっている。

【0071】なお図6では、サーバ装置20は1台しか示されていないが、複数台設けてもよい。同様に、クライアント装置30は、図6では1台しか示されていないが、複数台設けてもよい。

【0072】（セキュリティレベル）サーバ装置20及びクライアント装置30は、通信開始時に、それぞれ独立に設定したセキュリティレベルを相手に通知する。その後、サーバ装置20及びクライアント装置30は、互いのセキュリティレベルに基づいて定められるセキュリティレベルに従って通信する。

【0073】本実施形態では、前述したように、5段階のセキュリティレベルを設定可能であるが、それらのセキュリティレベルは以下になる。

セキュリティレベル“1”：暗号化も認証も行わない。いわゆる普通の通信である。

【0074】

セキュリティレベル“2”：暗号化だけを行う。

セキュリティレベル“3”：暗号化とユーザ認証を行う。

セキュリティレベル“4”：暗号化とサーバ認証を行う。なお、このセキュリティレベル“4”は、セキュリティレベル“3”と同等のセキュリティレベルである。

【0075】

セキュリティレベル“5”：暗号化、ユーザ認証及びサーバ認証を行う。

なお、サーバ装置20は、クライアント装置30が複数設けられている場合に、個々のクライアント装置30毎に独立したセキュリティレベルに従って通信することが可能である。

【0076】また、クライアント装置30は、サーバ装置20が複数設けられている場合に、個々のサーバ装置20毎に独立したセキュリティレベルに従って通信することが可能である。

【0077】そして、セキュリティレベルとしては、他に次のようなものを設定することも可能である。即ち、セキュリティレベル“2”～“5”で暗号化を行わないもの、クライアントを認証するもの等である。

【0078】さらに、ここでいうユーザ認証には、パスワードを用いた認証や公開鍵証明書を用いた認証が含まれる。本実施形態では、公開鍵証明書を用いた認証について説明する。

【0079】（サーバ装置20の構成）サーバ装置20は、ネットワーク40に接続された通信制御部21、この通信制御部21に接続されたサービス処理部22、このサービス処理部22に接続されたセキュリティレベル制御装置10、及びサービス処理部22に接続された記憶部23を備えて構成されている。

【0080】通信制御部21は、サーバ装置20がネットワーク40との間で通信を行うための制御を行う。サービス処理部22は、サーバ装置20内で発生するさまざまなサービス要求を実現するため、セキュリティレベル制御装置10、通信制御部21及び記憶部23との間でデータのやりとりを行う。

【0081】記憶部23は、ユーザの秘密鍵（SK_m：mは添字）、ユーザの証明書（CERT_m：mは添字）及び発行局の証明書（CERT_{ca}：caは添字）に関する情報を格納する。この記憶部23は、例えば、RAM（Random Access Memory）、半導体記憶装置、磁気ディスク記憶装置、磁気テープ装置、M/O（Magnet Optical：光磁気ディスク装置）、I/Cカード等が用いられる。

【0082】セキュリティレベル制御装置10は、通信開始時にクライアント装置30から通知されたセキュリティレベルと、サーバ装置20自体のセキュリティレベルとに基づいて、実際に行われる通信のセキュリティを制御する装置である。セキュリティレベル制御装置10の構成については、クライアント装置30の構成に続いて説明する。

【0083】（クライアント装置30の構成）クライアント装置30は、ネットワーク40に接続された通信制御部31、この通信制御部31に接続されたサービス処理部32、このサービス処理部32に接続されたセキュリティレベル制御装置10、及びサービス処理部32に接続された記憶部33を備えて構成されている。

【0084】通信制御部31は、サーバ装置20がネットワーク40との間で通信を行うための制御を行う。サービス処理部32は、クライアント装置30内で発生するさまざまなサービス要求を実現するため、セキュリティレベル制御装置10、通信制御部31及び記憶部33との間でデータのやりとりを行う。

【0085】記憶部33は、サーバの公開鍵(PKs:sは添字)、サーバの証明書(CERTs:sは添字)、サーバの秘密鍵(SKs:sは添字)及び発行局の証明書(CERTca:caは添字)に関する情報を格納する。この記憶部33は、例えば、RAM(Random Access Memory)、半導体記憶装置、磁気ディスク記憶装置、磁気テープ装置、M/O(Magnet Optical:光磁気ディスク)装置、ICカード等が用いられる。

【0086】セキュリティレベル制御装置10は、通信開始時にサーバ装置20から通知されたセキュリティレベルと、クライアント装置30自体のセキュリティレベルとの折り合いをつける装置である。

【0087】(セキュリティレベル制御装置10の構成)サーバ装置20に設けられたセキュリティレベル制御装置10及びクライアント装置30に設けられたセキュリティレベル制御装置10は、同様に構成されているので、以下、両者を区別せずにその構成を説明する。

【0088】セキュリティレベル制御装置10は、図7に示すように、制御部16、セキュリティレベル認識部11、セキュリティレベル変換テーブル部12、セキュリティレベル設定部14、セキュリティレベル通知部15、暗号処理部17及び認証処理部18を備えて構成されている。

【0089】制御部16は、サービス処理部22(サーバ装置20の場合)又はサービス処理部32に接続(クライアント装置30の場合)に接続されるとともに、セキュリティレベル認識部11、セキュリティレベル変換テーブル部12、セキュリティレベル読出部13、セキュリティレベル設定部14、セキュリティレベル通知部15、暗号処理部17及び認証処理部18に接続されている。そして、制御部16は、各部間のデータのやりとりを制御する。

【0090】セキュリティレベル認識部11は、通信先が通知してくるセキュリティレベルを認識する。セキュリティレベル変換テーブル部12は、ネットワークで利用される全サーバ及び全クライアントがとりうるセキュリティレベルを1~5の5段階とした場合に、どのサーバ、クライアントでも該テーブルを使用可能とするために、サーバのインデックスを1~5とするとともに、クライアントのインデックスを1~5としている。そして、セキュリティレベル変換テーブル部12は、実際に通信を行うサーバ、クライアントがそれぞれ要求するセキュリティレベルに基づき、計25のパターンの中からいずれか1つが得られるように構成されている。

【0091】図8には、本実施形態のセキュリティレベル変換テーブル部12が示されている。同図の場合、例えば、クライアントのセキュリティレベルが“2”で、サーバのセキュリティレベルが“4”ならば、実際に行われる通信のセキュリティレベルは“4”となる。なお、“×”となっている部分は、サーバ装置20及びク

ライアント装置30がそれぞれ設定したセキュリティレベルでは、通信が行えないことを意味する。即ち、セキュリティレベルを制御できない場合に相当する。

【0092】このように本実施形態のセキュリティレベル変換テーブル部12は、サーバが提供する情報を重要と考え、クライアントが要求するセキュリティレベルよりもサーバが要求するセキュリティレベルの方が高い場合に、サーバが要求するセキュリティレベルを優先するようなテーブルとして構成されている。

【0093】しかしながら、セキュリティレベル変換テーブル部12の構成はこれに限るものではなく、自装置が要求できるセキュリティレベルのみを第1のインデックスとし、かつ、相手装置がとりうる全セキュリティレベルを第2のインデックスとしてテーブルを構成してもよい。例えば、上述のネットワークにおいて、自装置がクライアントで、かつセキュリティレベルは1~3を要求することが可能であり、相手装置となるサーバがとりうるセキュリティレベルが1~5とすると、自装置のインデックス(3個)×サーバのインデックス(5個)=計15個のパターンのなかからいずれか一つが得られるようにすればよい。

【0094】セキュリティレベル読出部13は、セキュリティレベル認識部11で認識された通信先のセキュリティレベル及びセキュリティレベル制御装置10側のセキュリティレベルをインデックスとして、このインデックスに対応するセキュリティレベルを前記セキュリティレベル変換テーブル部12から読み出す。

【0095】セキュリティレベル設定部14は、セキュリティレベル読出部13から読み出されたセキュリティレベルをセキュリティレベル制御装置10側のセキュリティレベルとして設定する。

【0096】セキュリティレベル通知部15は、自分のセキュリティレベルを通信先に通知する。暗号処理部17は、通信先に出力するメッセージを暗号化したり、逆に、通信先から入力された暗号化済みのメッセージを復号化する。なお、本実施形態では、慣用鍵暗号方式(共通鍵方式)としてDES(Data Encryption Standard)方式が用いられており、また、公開鍵暗号方式としてRSA方式(Rivest-Shamir-Aldeman)が用いられている。

【0097】認証処理部18は、サーバ認証を行ったり(クライアント装置30の場合)、ユーザ認証を行ったりする。

(実施形態におけるクライアント装置30及びサーバ装置20間の処理シーケンス)次に、図9及び図10を参照して、実施形態におけるクライアント装置30及びサーバ装置20間の処理シーケンス例を説明する。なお、ここで説明する処理シーケンスは、その全てが実行されるわけではなく、セキュリティレベル毎に必要な部分のみ実行される。

【0098】まず、クライアント装置30は、サーバ装

置20に通信要求を通知する(ステップ901。この通知を(1)で表す)。この通信要求に対して、サーバ装置20は、クライアント装置30にアクセプトを通知する(ステップ902。この通知を(2)で表す)。

【0099】クライアント装置30にアクセプトが通知された後、クライアント装置30及びサーバ装置20間で、通信の前処理が行われる(ステップ903。この前処理を(3)で表す)。ここで、通信の前処理とは、例えば、端末型情報、表示方法情報(何行、何桁で表示するか)、使用文字コード種別情報、IPアドレス等の情報交換を行うことをいう。

【0100】通信の前処理が終了した後、クライアント装置30は、クライアント装置30が設定したセキュリティレベルをサーバ装置20に通知する(ステップ904。この通知を(4)で表す)。この通知により、サーバ装置20は、クライアント装置30が設定したセキュリティレベルを認識する(ステップ905。この認識を(6)で表す)。

【0101】続いて、サーバ装置20は、サーバ装置20が設定したセキュリティレベルをクライアント装置30に通知する(ステップ906。この通知を(5)で表す)。この通知により、クライアント装置30は、サーバ装置20が設定したセキュリティレベルを認識する(ステップ907。この認識を(7)で表す)。

【0102】クライアント装置30は、クライアント装置30側で設定したセキュリティレベルとサーバ装置20から通知されたセキュリティレベルに従って、実際に行われる通信のセキュリティレベルを選択する(ステップ908。この選択を(8)で表す)。また、サーバ装置20は、サーバ装置20側で設定したセキュリティレベルとクライアント装置30から通知されたセキュリティレベルに従って、実際に行われる通信のセキュリティレベルを選択する(ステップ909。この選択を(8)で表す)。

【0103】ここで、ステップ908及びステップ909で選択されるセキュリティレベルは、互いに一致する。その後、クライアント装置30は、ユーザの証明書(CERTm)をサーバ装置20に通知する(ステップ910。この通知を(A)で表す)。

【0104】サーバ装置20は、通知されたユーザの証明書を発行局の証明書(CERTca)で検証する(ステップ911)。また、サーバ装置20は、サーバの公開鍵(PKs)又はサーバの証明書(CERTs)をクライアント装置30に通知する(ステップ912。この通知を(B)で表す)。

【0105】クライアント装置30は、通知されたサーバの証明書(CERTs)を発行局の証明書(CERTca)で検証する(ステップ913)。また、クライアント装置30は、認証(ここでは、サーバの認証)を行う種であるDEK1を乱数により生成する(ステップ914)。

【0106】その後、クライアント装置30は、サーバの公開鍵(PKs)でDEK1を暗号化することにより生成したPKs(DEK1)をサーバ装置20に通知する(ステップ915。この通知を(C)で表す)。つまり、発信者であるクライアント装置30は、本文を読むための共通の暗号鍵(共通鍵)を、受信者であるサーバ装置20の公開鍵(PKs)で暗号化して通知する。ここまでの処理段階では、クライアント装置30及びサーバ装置20に共通の暗号鍵(共通鍵)が無い場合、暗号化は、公開鍵暗号方式(RSA方式)で行われる。

【0107】サーバ装置20は、通知されたPKs(DEK1)をサーバの秘密鍵(SKs)で復号化することによりDEK1を取り出す(ステップ916)。つまり、受信者であるサーバ装置20は、自分の秘密鍵であるサーバの秘密鍵(SKs)で共通鍵を復号化する。その後、クライアント装置30から送られる本文は、復号された共通鍵で復号化される。

【0108】また、サーバ装置20は、サーバの秘密鍵(SKs)を用いてDEK1を行うことによりSKs(DEK1)を生成する(ステップ917)。その後、サーバ装置20は、SKs(DEK1)をDEK1で暗号化することにより生成したDEK1(SKs(DEK1))をクライアント装置30に通知する(ステップ918。この通知を(D)で表す)。ここで、SKs(DEK1)をDEK1で暗号化するのは、電子署名を盗聴されないためである。また、電子署名は、発信者(ユーザ)の認証と本文内容に改竄が行われていないことを検証するために行われる。例えば、署名者Aは、適切な関数を使って本文のダイジェストを作り、それをAの秘密鍵を用いて暗号化する。これが署名となる。検証者Bは、署名者Aの公開鍵を用いて署名を元に戻し、その結果が原本の本文のダイジェストに等しいかを調べる。等しくなければ、本文は改竄されていることが分かる。

【0109】ここで、クライアント装置30は、処理Pとして、以下の1)~3)を行う(ステップ919)。1) DEK1(SKs(DEK1))を復号化してSKs(DEK1)を取り出す。2) 取り出されたSKs(DEK1)からサーバの証明書の中の公開鍵(PKs)を用いて、DEK1を取り出す。3) 取り出されたDEK1とステップ914で生成されたDEK1とを比較する。この比較により、サーバの認証が行われることになる。この認証が行われるのは、サーバの証明書として公開されている鍵が本当にサーバ装置20のものかどうかを確認するためである。この確認は、第三者機関が認証するサーバの証明書(CERTs)を用いて行われる。このような確認は、第三者認証あるいは電子公証人とも呼ばれている。簡単に言うと、自分が送ったものに対し相手に署名をしてもらい、その署名を相手の公開鍵でほどいた結果が自分の送ったものと同一であれば、認証ができたことになるということである。

【0110】クライアント装置30は、ステップ919の3)の比較の結果、同じであればサーバ装置20にAC

K を通知し、異なっていればサーバ装置 20 に NACK を通知する (ステップ 920)。

【0111】次に、サーバ装置 20 は、認証 (ここでは、ユーザの認証) を行う種である DEK2 を乱数により生成する (ステップ 921)。その後、サーバ装置 20 は、慣用暗号化方式を用いて DEK2 を暗号化することにより生成した DEK1 (DEK2) をクライアント装置 30 に通知する (ステップ 922。この通知を (F) で表す)。ここで、慣用暗号化方式が用いられる理由は、クライアント装置 30 及びサーバ装置 20 に暗号鍵 DEK1 が共有化されていることと、その暗号鍵 DEK1 を用いると処理速度が速くなるためである。いいえかれば、すべてを公開鍵で行うと計算量が膨大になることに原因して処理速度が落ちるのを防ぐためである。

【0112】次に、クライアント装置 30 は、サーバ装置 20 から通知された DEK1 (DEK2) をユーザの秘密鍵 (SKm) で復号化することにより DEK2 を取り出す (ステップ 923)。

【0113】また、クライアント装置 30 は、ユーザの秘密鍵 (SKm) を用いて DEK2 に対して電子署名を行うことにより SKm (DEK2) を生成する (ステップ 924)。その後、クライアント装置 30 は、SKm (DEK2) を DEK2 で暗号化することにより生成した DEK2 (SKm (DEK2)) を通知する (ステップ 925。この通知を (G) で表す)。

【0114】ここで、サーバ装置 20 は、処理 Q として、以下の 1) ~ 3) を行う (ステップ 926)。1) DEK2 (SKm (DEK2)) を復号化して SKm (DEK2) を取り出す。2) 取り出された SKm (DEK2) からユーザの秘密鍵 (SKm) を用いて DEK2 を取り出す。3) 取り出された DEK2 とステップ 921 で生成された DEK2 とを比較する。この比較により、ユーザの認証が行われることになる。

【0115】サーバ装置 20 は、ステップ 926 の 3) の比較の結果、同じであればクライアント装置 30 に ACK を通知し、異なっていればクライアント装置 30 に NACK を通知する (ステップ 927。この通知を (H) で表す)。

【0116】その後、クライアント装置 30 及びサーバ装置 20 間で、暗号鍵 DEK2 を用いた通信が行われる (ステップ 928。この通信を (9) で表す)。

(各セキュリティレベルで行われる処理シーケンス) 次に、各セキュリティレベルで行われる処理シーケンスを図 11 を参照して説明する。

【0117】まず、セキュリティレベル “1” では、前述した (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8) 及び (9) の動作が順に処理が行われる。

【0118】また、セキュリティレベル “2” では、前述した (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(B)、(C) 及び (F) の動作が順に処理が行われる。

【0119】そして、セキュリティレベル “3” では、前述した (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(A)、(B)、(C)、(F)、(G) 及び (H) の動作が順に処理が行われる。

【0120】そして、セキュリティレベル “4” では、前述した (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(B)、(C)、(D)、(E) 及び (F) の動作が順に処理が行われる。

【0121】そして、セキュリティレベル “5” では、前述した (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、(A)、(B)、(C)、(D)、(E)、(F)、(G) 及び (H) の動作が順に処理が行われる。

【0122】(処理動作例その 1) 次に、図 12 を参照して、処理動作例その 1 の処理動作を説明する。まず、クライアント装置 30 (クライアント) が通信先にアクセスする (ステップ 1201)。

【0123】次に、サーバ装置 20 (サーバ) がクライアントの通信をアクセプトする (ステップ 1202)。ここで、通信の前処理が完了する (ステップ 1203)。

【0124】次に、クライアントがセキュリティレベル “3” を要求する (ステップ 1204)。この要求により、サーバのセキュリティレベル制御装置 10 は、クライアントのセキュリティレベルを “3” と認識する (ステップ 1205)。

【0125】次に、サーバがセキュリティレベル “5” を要求する (ステップ 1206)。この要求により、クライアントのセキュリティレベル制御装置 10 は、サーバのセキュリティレベルを “5” と認識する (ステップ 1207)。

【0126】ここで、サーバ及びクライアントのセキュリティレベル制御装置 10 は、セキュリティレベル変換テーブル部 12 に従って、セキュリティレベル “5” を選択する (ステップ 1208)。

【0127】サーバ及びクライアントは、図 9 及び図 10 の (A)、(B)、(C)、(D)、(E)、(F)、(G) 及び (H) の処理シーケンスと暗号鍵の交換を実行した後、暗号化通信を行う (ステップ 1209)。

【0128】(処理動作例その 2) 次に、図 13 を参照して、処理動作例その 2 の処理動作を説明する。まず、クライアント装置 30 (クライアント) が通信先にアクセスする (ステップ 1301)。

【0129】次に、サーバ装置 20 (サーバ) がクライアントの通信をアクセプトする (ステップ 1302)。ここで、通信の前処理が完了する (ステップ 1303)。

【0130】次に、クライアントがセキュリティレベル

“2”を要求する(ステップ1304)。この要求により、サーバのセキュリティレベル制御装置10は、クライアントのセキュリティレベルを“2”と認識する(ステップ1305)。

【0131】次に、サーバがセキュリティレベル“2”を要求する(ステップ1306)。この要求により、クライアントのセキュリティレベル制御装置10は、サーバのセキュリティレベルを“2”と認識する(ステップ1307)。

【0132】ここで、サーバ及びクライアントのセキュリティレベル制御装置10は、セキュリティレベル変換テーブル部12に従って、セキュリティレベル“2”を選択する(ステップ1308)。

【0133】サーバ及びクライアントは、図9及び図10の(B)、(C)及び(F)の処理シーケンスと暗号鍵の交換を実行した後、暗号化通信を行う(ステップ1309)。

【0134】(本実施形態の効果)以上説明したように、本実施形態では、相手装置の要求レベルだけに基いて通信のレベルを決めるのではなく、双方の装置の要求レベルにより実際の通信のレベルを決めるようにしたため、以下のような効果を生じる。即ち、インターネットに本実施例を適用した場合に、サーバとユーザの装置(インターネットの世界ではホストと呼ばれる)間で通信を行う場合に、サーバは、提供する情報を暗号化して他の装置に参照させないようにしたいのに対し、ユーザが平文での通信を要求するような場合でも、セキュリティレベル変換テーブル部12を、サーバの要求レベルが優先されるように構成しておくことで、問題が生じるようなことがなくなる。

【0135】

【発明の効果】本発明の第1のセキュリティレベル制御装置及び第1から第4のネットワーク通信システムによれば、セキュリティレベル認識部で認識されたセキュリティレベルをセキュリティレベル制御装置側のセキュリティレベルとして設定するようにしたので、通信先との間で予めセキュリティレベルを決定しておくことなく通信を行うことを可能となる。

【0136】本発明の第2のセキュリティレベル制御装置及び第5から第10のネットワーク通信システムによれば、通信先から通知されたセキュリティレベルと、セキュリティレベル制御装置が設けられる側のセキュリティレベルとに基づいて、セキュリティレベルを設定するようにしたので、自分のセキュリティレベルを反映させた通信を行うことを可能となる。

【図面の簡単な説明】

【図1】本発明の第1のセキュリティレベル制御装置に対応した原理ブロック図である。

【図2】本発明の第2のセキュリティレベル制御装置に対応した原理ブロック図である。

【図3】本発明の第1のネットワーク通信システムに対応した原理ブロック図である。

【図4】本発明の第2のネットワーク通信システムに対応した原理ブロック図である。

【図5】本発明の第9のネットワーク通信システムに対応した原理ブロック図である。

【図6】実施形態のシステム構成図である。

【図7】実施形態のセキュリティレベル制御装置の構成ブロック図である。

【図8】実施形態のセキュリティレベル制御装置が有するセキュリティレベル変換テーブル部を示す図である。

【図9】実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例(その1)を示す図である。

【図10】実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例(その2)を示す図である。

【図11】実施形態の各セキュリティレベルで行われる処理シーケンスを示す図である。

【図12】実施形態における処理動作例その1の処理フローチャートを示す図である。

【図13】実施形態における処理動作例その2の処理フローチャートを示す図である。

【符号の説明】

10・・・セキュリティレベル制御装置(セキュリティレベル制御部)

11・・・セキュリティレベル認識部

12・・・セキュリティレベル変換テーブル

13・・・セキュリティレベル読出部

14・・・セキュリティレベル設定部

15・・・セキュリティレベル通知部

16・・・制御部

17・・・暗号処理部

18・・・認証処理部

20・・・サーバ装置

30・・・クライアント装置

31・・・通信制御部

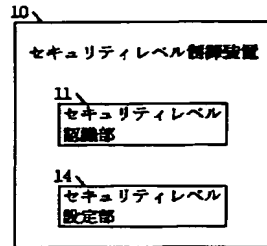
32・・・サービス処理部

33・・・記憶部

40・・・ネットワーク

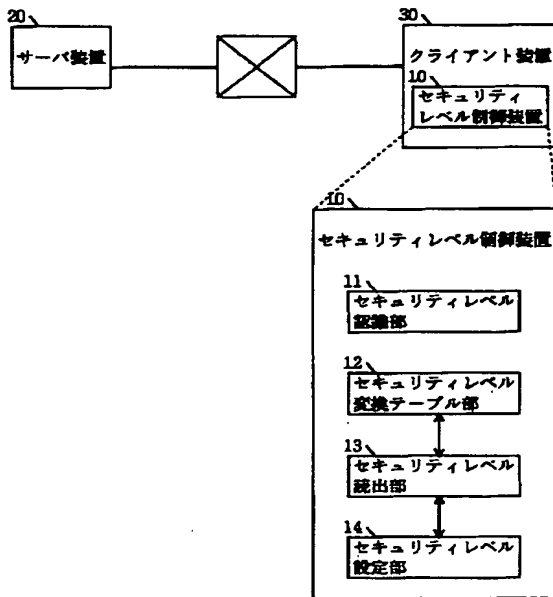
【図 1】

本発明の第1のセキュリティレベル制御装置に対応した原理ブロック図



【図 3】

本発明の第1のネットワーク通信システムに対応した原理ブロック図



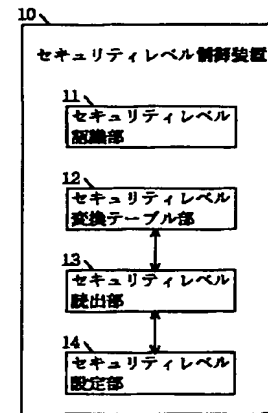
【図 8】

実施形態のセキュリティレベル制御装置が有するセキュリティレベル変換テーブル部を示す図

サーバのセキュリティレベル クライアントのセキュリティレベル	1	2	3	4	5
1	1	2	×	4	×
2	2	2	×	4	×
3	×	2	3	×	5
4	×	×	×	4	×
5	×	×	×	4	5

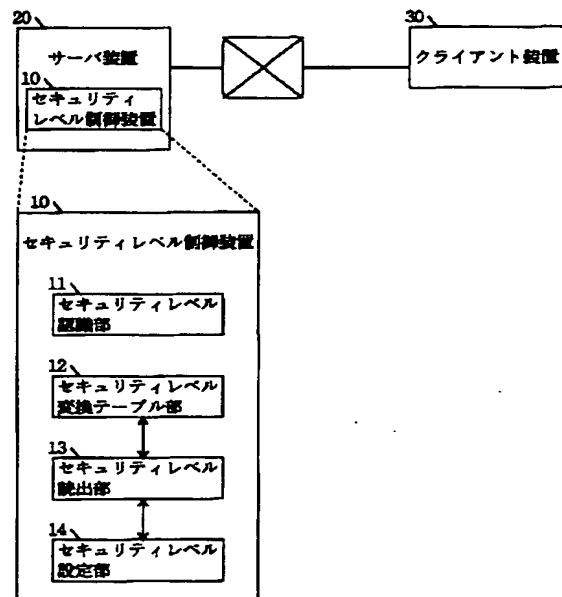
【図 2】

本発明の第2のセキュリティレベル制御装置に対応した原理ブロック図



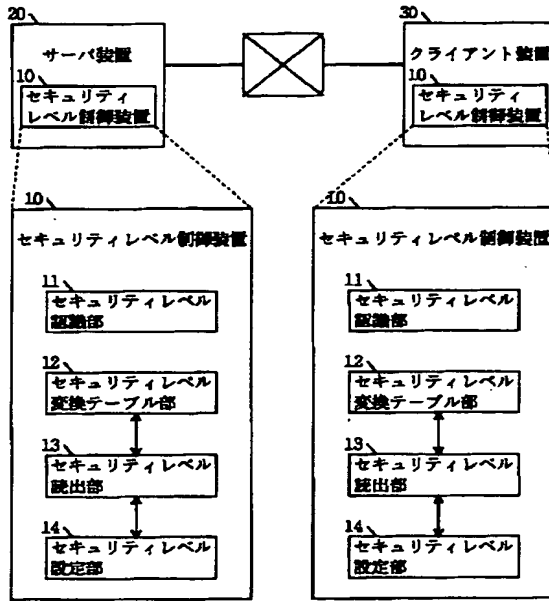
【図 4】

本発明の第2のネットワーク通信システムに対応した原理ブロック図



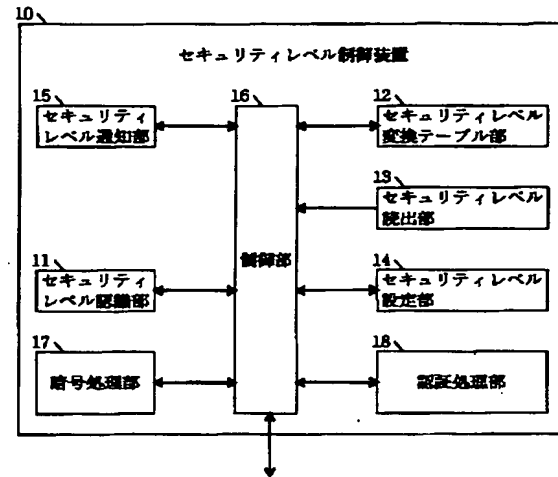
【図 5】

本発明の第9のネットワーク通信システムに対応した処理ブロック図



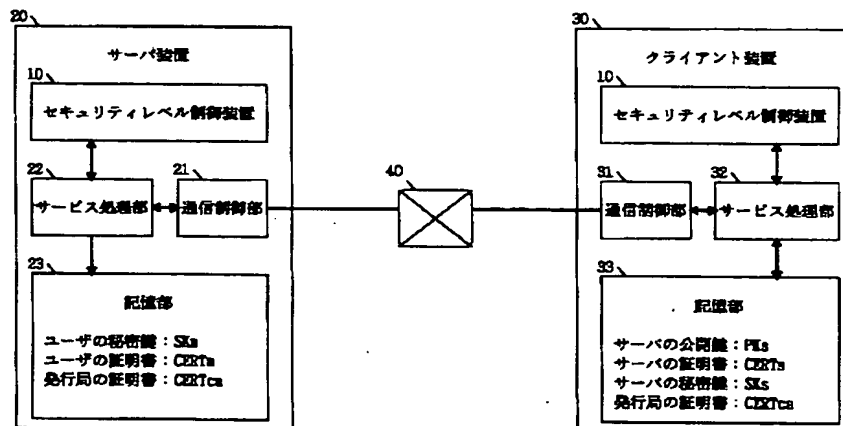
【図 7】

実施形態のセキュリティレベル制御装置の構成ブロック図



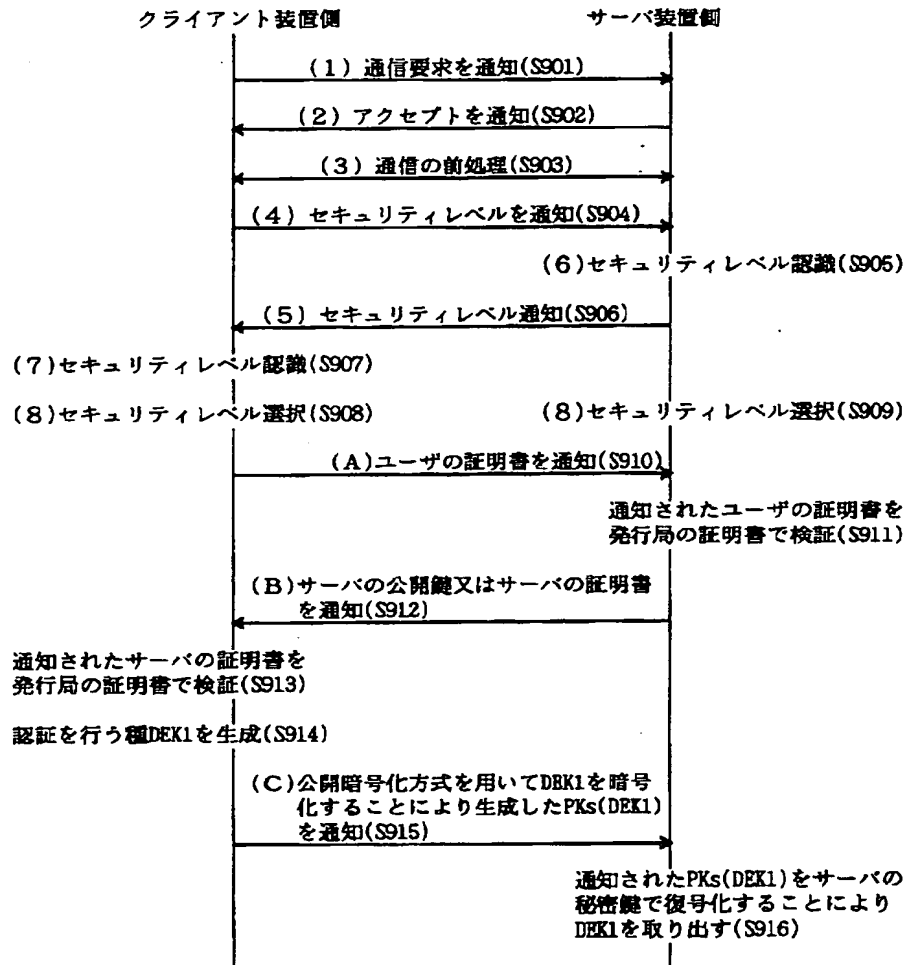
【図 6】

実施形態のシステム構成図



【図 9】

実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その1）



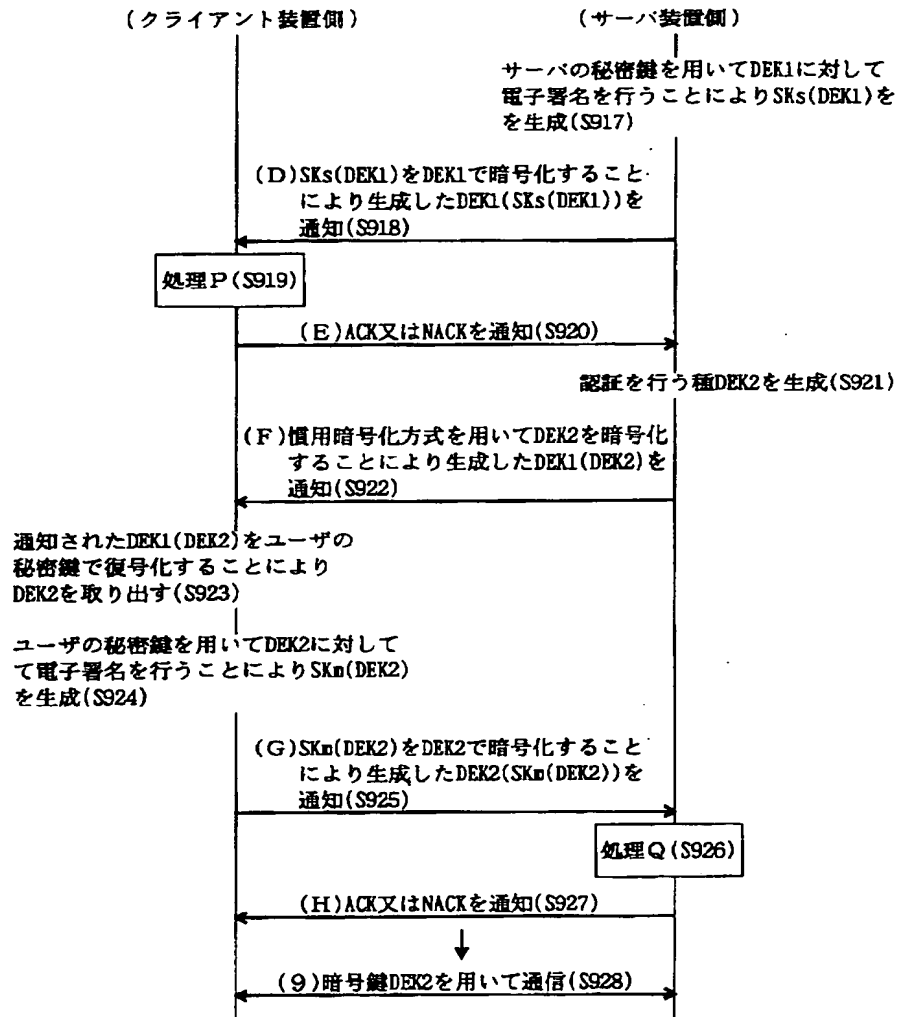
【図 11】

実施形態の各セキュリティレベルで行われる処理シーケンス

セキュリティ レベル "1"	(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(9)
セキュリティ レベル "2"	(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(F)
セキュリティ レベル "3"	(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(F)→(G)→(H)
セキュリティ レベル "4"	(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(D)→(E)→(F)
セキュリティ レベル "5"	(1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(D)→(E)→(F)→(G)→(H)

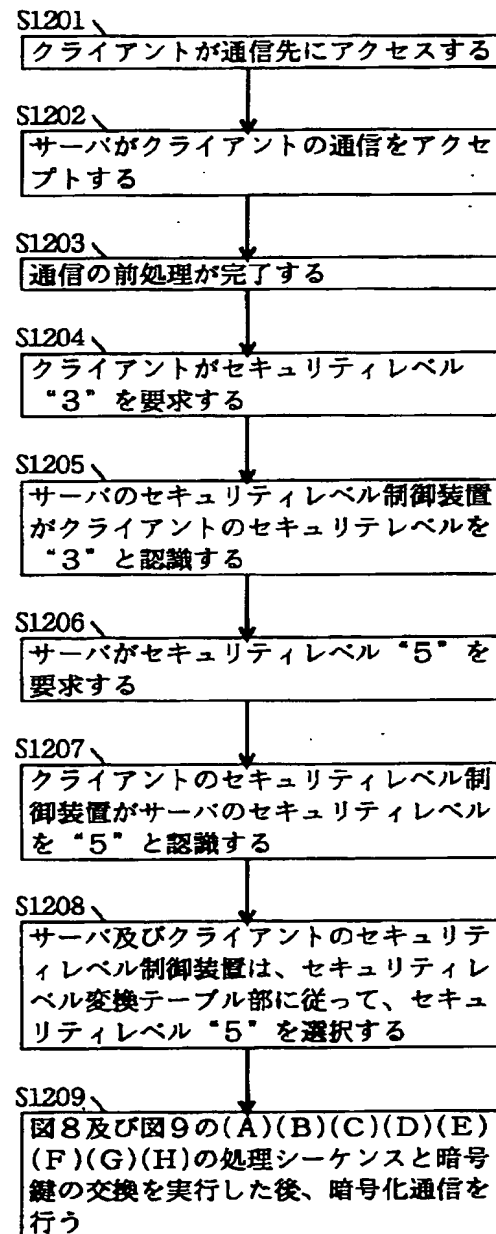
【図 10】

実施形態におけるクライアント装置及びサーバ装置間の処理シーケンス例（その2）



【図 12】

実施形態における処理動作例その 1 の処理フローチャート



【図 13】

実施形態における処理動作例その2の処理フローチャート

